

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

UNITED STATES OF AMERICA,	§	
	§	
v.	§	CRIMINAL CASE NO. 3:23-CR-0205-B
	§	
SEAN MICAH JORDAN,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION & ORDER

Before the Court is Defendant Sean Micah Jordan's Motion to Suppress and Motion for a *Franks* Hearing (Doc. 34). For the following reasons, the Motion is **DENIED**.

I.

BACKGROUND

The Government charges Jordan with possession and receipt of child sexual abuse materials ("CSAM"), in violation of 18 U.S.C. § 2252. Doc. 1, Indictment. Task Force Officer ("TFO") Brandon Poor determined that Jordan had likely downloaded CSAM during an investigation of CSAM trafficking on Freenet. Doc. 34, Affidavit, 15–19.<sup>1</sup>

Freenet is an open-source software that allows users to anonymously share, request, and download encrypted files. *Id.* at 7–8. When a user installs Freenet, she agrees to provide Freenet storage space on her computer's hard drive. *Id.* at 8. When a user uploads a file to Freenet, the software breaks the file into pieces, encrypts each piece, and distributes the pieces randomly to different users' hard drives throughout the Freenet network. *Id.*

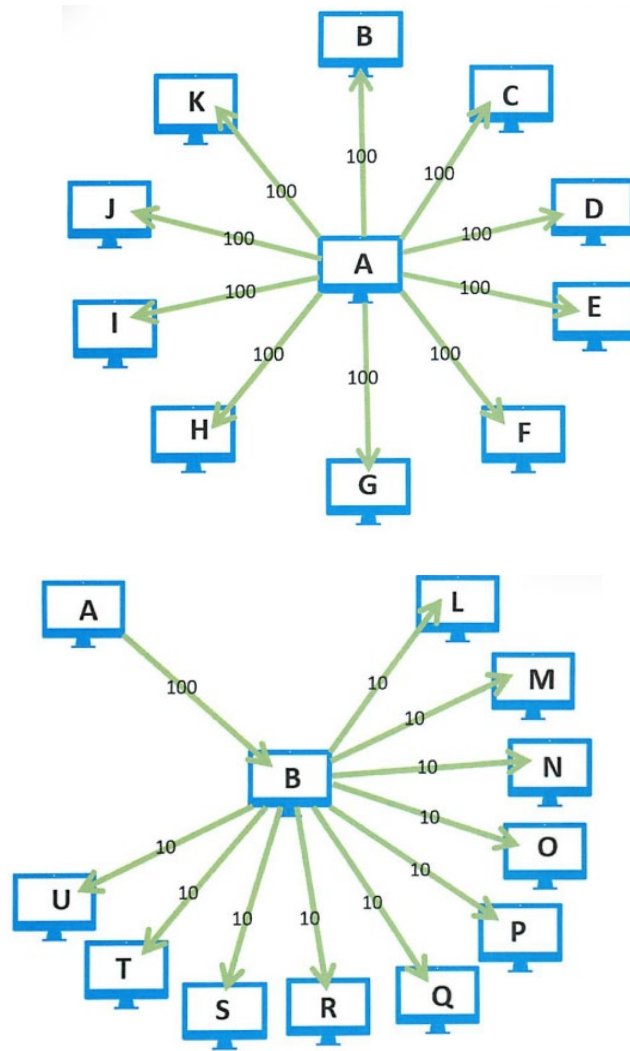
---

<sup>1</sup> Jordan attached the Affidavit to his Motion. When citing to the Affidavit, the Court refers to the Affidavit's pagination. But when citing to other exhibits attached to Jordan's Motion (Doc. 34), the Court refers to ECF pagination.

When Freenet breaks up a file, it creates an index that lists all the pieces of the file. *Id.* It also creates a unique key—a series of letters, numbers, and characters—that a user uses to download the file. *Id.* There is no search function in Freenet. Instead, a user can only find and download a file by using that file’s unique key. *Id.* at 8, 12.

Freenet users are connected to “peers,” or other Freenet users, creating a network. When a user requests to download a particular file using a unique key, Freenet’s software requests all the pieces of the file from the user’s network of peers. *Id.* at 9. But the Freenet software does not ask every peer for every piece of the requested file. Instead, it divides requests for the various pieces of the file among the user’s peers. *Id.* If one peer’s hard drive does not contain the requested pieces, that peer sends the request to one of its peers. *Id.* When a peer relays a request, the request is then divided up into a smaller number of pieces and distributed among that peer’s peers. *Id.*

For example, if user A enters the key for file Y, Freenet would send a request for the pieces of file Y to A’s peers. Freenet might request 100 pieces from user B, one of A’s peers. If B does not have any pieces of the file, B sends a request to B’s peers. B would not ask each peer for every piece requested by A. Instead, B would break up the request it received for 100 pieces of file Y. For example, B’s peer L might receive a request for 10 pieces, B’s peer M might receive a request for 10 pieces, and so on. The pieces are not necessarily distributed evenly among users. This example is depicted below.



*Id.* at 9–10.

If B’s peers do not have pieces of the file, the request is relayed to other users’ peers until the request either reaches a peer who has the requested pieces of the file, or the request expires. *Id.* at 10. Each request is forwarded to peers only a limited number of times, which is called a hops-to-live (“HTL”) number. *Id.* at 10; Doc. 34, Mot., 7. After the request reaches its HTL number, the request expires. *Id.* The default HTL number is either 17 or 18. Doc. 34, Affidavit, 10–11. In other words, if a user does not change Freenet’s default settings, then when she requests a file, the request will forward to peers 17 or 18 times at the most. Freenet randomizes the default HTL number between

17 or 18 to preserve anonymity. *Id.* at 11. If the HTL number were the same every time—and not randomized—then the HTL number would reveal whether a file request came from the original requestor. *Id.* Because of Freenet’s randomization and a user’s ability to change their default HTL number, a peer cannot be certain whether a request they receive is from an original requestor or a user relaying someone else’s request. Doc. 34, Mot., 8.

Law enforcement officers have been investigating CSAM trafficking on Freenet since 2011. Doc. 34, Affidavit, 13. Law enforcement officers use a modified version of Freenet that is identical to a normal user’s version except that it automatically records information about requests that the law enforcement’s computer receives from peers. *Id.* After recording information about requests, law enforcement can use an algorithm to determine if it is statistically likely that a particular request was made by an original requestor instead of a mere relayor (i.e., one of the requestor’s peers). *Id.* at 14. The algorithm was developed by computer scientists and uses a mathematical formula. *Id.* at 15, Doc. 34, Ex. B, 68. The algorithm is “highly accurate” and has a high true positive rate and low false positive rate. Doc. 34, Affidavit, 15.

In 2023, TFO Poor was investigating CSAM on Freenet when he determined that Jordan’s IP address likely requested CSAM. *Id.* Three separate requests from the same IP address requested many pieces of files known to be CSAM. *Id.* at 16–17. TFO Poor also found the same IP address made three requests for many pieces of files known to be CSAM during a 2021 investigation. *Id.* at 17–18. TFO Poor determined the IP address belongs to Sean Micah Jordan and applied for a warrant to search Jordan’s house and cars for evidence of CSAM. *Id.* at 19–20, 42. A magistrate judge granted the search warrant application. *See id.* at 1.

Jordan filed a Motion to Suppress and Motion for a *Franks* hearing challenging the sufficiency of TFO Poor's affidavit that he used to obtain the search warrant. The Court considers his Motion below.

## II.

### LEGAL STANDARD

The Fourth Amendment of the United States Constitution guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation.” U.S. CONST. amend. IV. “To supplement the bare text, [the Supreme Court] created the exclusionary rule, a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation.” *Davis v. United States*, 564 U.S. 229, 231–32 (2011). The focus of the rule is “not on restoring the victim to his rightful position but on deterring police officers from knowingly violating the Constitution.” *United States v. Wallace*, 885 F.3d 806, 810 (5th Cir. 2018) (quoting *United States v. Allen*, 625 F.3d 830, 836 (5th Cir. 2010)). “Thus, application of the rule is ‘not a personal constitutional right.’ Nor is it automatic in the face of a Fourth Amendment violation.” *United States v. Ganzer*, 922 F.3d 579, 584 (5th Cir. 2019) (first quoting *Davis*, 564 U.S. at 236 and then citing *Herring v. United States*, 555 U.S. 135, 140 (2009)).

Therefore, “[t]he proponent of a motion to suppress has the burden of proving, by a preponderance of evidence, that the evidence in question was obtained in violation of his Fourth Amendment rights.” *United States v. Garcia*, 99 F.4th 253, 267 (5th Cir. 2024) (quoting *United States v. Smith*, 978 F.2d 171, 176 (5th Cir. 1992)). “[T]he Fourth Amendment entitles a defendant to a hearing on the veracity of a warrant affidavit if he can make a sufficient preliminary showing that

the affiant officer obtained the warrant by recklessly including material falsehoods in a warrant application.” *Melton v. Phillips*, 875 F.3d 256, 262 (5th Cir. 2017) (quoting *Franks v. Delaware*, 438 U.S. 154, 171-72 (1978)).

### III.

#### ANALYSIS

The Court **DENIES** Jordan’s Motion to Suppress and Motion for a *Franks* Hearing. First, Jordan is not entitled to a *Franks* hearing because he failed to show TFO Poor’s affidavit contained a material omission. Second, Jordan’s Motion to Suppress is denied because the good faith exception applies.

A. *Jordan’s Motion for a Franks Hearing is Denied.*

First, the Court denies Jordan’s Motion for a *Franks* hearing. The purpose of a *Franks* hearing is to determine the truthfulness of an affidavit supporting a warrant. *See Franks*, 438 U.S. at 171. But an affidavit is presumed to be valid. *Id.* Therefore, to qualify for a *Franks* hearing, a defendant must make a preliminary showing that: (1) an affidavit contained a falsehood; (2) the falsehood was made deliberately or with reckless disregard for the truth; and (3) the affidavit would fail to establish probable cause if the false statement were excised. *United States v. Ortega*, 854 F.3d 818, 826 (5th Cir. 2017). So even if a defendant shows that an affidavit supporting a warrant contained a deliberate or reckless falsehood, “he is not entitled to a hearing if,” absent the falsehood, “there remains sufficient content in the warrant affidavit to support a finding of probable cause.” *United States v. Brown*, 298 F.3d 392, 395-96 (5th Cir. 2002) (citation omitted).

Jordan is not entitled to a *Franks* hearing because he did not make a preliminary showing that TFO Poor’s affidavit contained deliberate or reckless falsehoods. Jordan argues he is entitled to

a *Franks* hearing because TFO Poor's affidavit omitted information about the algorithm used to identify Jordan as the requestor of CSAM. Doc. 34, Mot., 5–16. A material omission can qualify as a false statement. See *United States v. Kendrick*, 980 F.3d 432, 441 (5th Cir. 2020). “To determine whether facts omitted from a warrant affidavit are material to the determination of probable cause, courts ordinarily insert the omitted facts into the affidavit and ask whether the reconstructed affidavit would still support a finding of probable cause.” *Marks v. Hudson*, 933 F.3d 481, 487–88 (5th Cir. 2019). An “affiant’s failure to describe every element of his reasoning process, without more, should not be deemed a material omission.” *United States v. Mueller*, 902 F.2d 336, 342 (5th Cir. 1990).

Here, none of the omissions Jordan identifies are material because if each alleged omission were inserted into the affidavit, the “affidavit would still support a finding of probable cause.” See *Marks*, 933 F.3d at 487–88. First, Jordan quotes an article to explain that “it is not possible to determine the originator of a request simply from the HTL number.” Doc. 34, Mot., 8. But the affidavit does not rely on the HTL number alone, so including this would not destroy probable cause. And the article Jordan quotes was published before the algorithm was developed, so it has little bearing on the affidavit’s description of the algorithm. See Doc. 37, Resp., 24.

Next, Jordan asserts the “affidavit omitted the fact that the algorithm itself assumes that the peer is the original requestor or a directly connected peer of the peer.”<sup>2</sup> Doc. 34, Mot., 8. But the affidavit explains that law enforcement officers only analyze requests that may be forwarded 17 or

---

<sup>2</sup> Jordan later says that the algorithm assumed Jordan *was the original requestor*, rather than *the original requestor or a directly connected peer*. See *id.* at 10, 15. Based on the paper explaining the algorithm, which Jordan attaches to his Motion, Jordan’s first assertion was accurate, i.e., the algorithm assumed Jordan was *either* the original requestor *or* a directly connected peer. See Doc. 34, Ex. B, 71 (“[T]he technique assumes that either the peer is the downloader or a directly connected peer of the peer is the downloader.”).

18 times. Doc. 34, Affidavit, 14. In other words, law enforcement officers only analyze file requests that were made by the original requestor or the first relayer, *unless* the requestor increased Freenet's default HTL to more than 18. Thus, law enforcement officers only use HTL numbers for the original requestor or direct peer of the requestor in the algorithm during investigations, unless a user changes the HTL number. As a result, including this assumption in the affidavit would not destroy probable cause because the algorithm's assumption largely conforms to the reality of investigations.

Jordan also argues the affidavit omitted that one of the algorithm's four variables—the number of peers the subject user has—is unknowable, and the algorithm assumes it is eight. *Id.* at 11. And the affidavit omitted that the algorithm assumes “that the block requests are a random, uniform distribution,” when “Freenet's routing mechanisms do not result in a uniform distribution of requests such that the block requests would be even from all peers.” Doc. 42, Reply, 2–3. But neither details about the algorithm's assumption of a variable, nor the fact that block requests are unevenly distributed, defeat probable cause. *See id.* at 4, 11; Doc. 42, Reply, 23. Even with the algorithm's assumptions, TFO Poor attests it is “highly accurate.” Doc. 34, Affidavit, 15.

Moreover, TFO Poor was not required to include each of the algorithm's assumptions and details to support a finding of probable cause. *See United States v. Gonzalez*, No. 5:18-CR-482, 2018 WL 6174202, at \*9 (S.D. Tex. Nov. 7, 2018), *report and recommendation adopted*, 2018 WL 6173724 (S.D. Tex. Nov. 26, 2018) (explaining an “affidavit need only detail the functionality of the software” used to identify likely downloaders of CSAM). Jordan argues that the affidavit does not “apply nor describe how [TFO Poor] applied the mathematical formula” or “how the data obtained . . . establishes probable cause that Mr. Jordan was the original requestor as opposed to a peer relaying a request.” Doc. 34, Mot., 4. Jordan further argues TFO Poor omitted key parts about the algorithm,



“despite attesting to his personal knowledge of the leading academic paper discussing it.” *Id.* at 6. Finally, he argues the affidavit said that “the algorithm showed [Jordan] was a downloader . . . in a conclusory manner.” *Id.* at 10.

But “the Affidavit provides substantial detail as to [the algorithm’s] functionality and . . . use.” *Gonzalez*, 2018 WL 6174202, at \*9. The affidavit explains that law enforcement applies a mathematical formula “to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.” Doc. 34, Affidavit, 14. The affidavit notes that a mere relayor would request fewer pieces of the file than would the original requestor. *Id.* Moreover, it explains that the formula is “highly accurate” with a “low false positive rate,” that dozens of similar law enforcement searches have found CSAM evidence, and that the officer would provide the academic paper detailing the algorithm upon the court’s request. *Id.* at 15. And everything discussed above rebuts Jordan’s contention that the affidavit stated that Jordan was a downloader in a conclusory manner. Doc. 34, Mot., 10. TFO Poor’s omissions of details about the algorithm were not material. See *Mueller*, 902 F.2d at 342. Accordingly, Jordan is not entitled to a *Franks* hearing.

*B. Jordan’s Motion to Suppress is Denied.*

Next, the Court denies Jordan’s Motion to Suppress. The court analyzes a motion to suppress evidence obtained under a search warrant in two steps. *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003); see also *United States v. Simpson*, No. 3:09-CR-249-D-06, 2011 WL 721912, at \*3 (N.D. Tex. Mar. 2, 2011) (Fitzwater, C.J.). First, the court determines whether the good-faith exception to the exclusionary rule applies. *Payne*, 341 F.3d at 399 (citing *United States v. Pena-Rodriguez*, 110 F.3d 1120, 1129–30 (5th Cir. 1997)). If it does, the court “need not reach the question of probable cause

for the warrant unless it presents a ‘novel question of law,’ resolution of which is ‘necessary to guide future action by law enforcement officers and magistrates.’” *Id.* (quoting *Pena-Rodriguez*, 110 F.3d at 1130 n.10). Second, if the good-faith exception does not apply, the court determines whether “the magistrate judge had a substantial basis for concluding that probable cause existed.” *United States v. Lampton*, 158 F.3d 251, 258 (5th Cir. 1998) (quotation omitted).

“Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers’ reliance on the warrant was objectively reasonable and in good faith.” *Payne*, 341 F.3d at 399. The good-faith exception “does not apply if the warrant affidavit contains a false statement that was made intentionally or with reckless disregard for its truth.” *United States v. Cavazos*, 288 F.3d 706, 709–10 (5th Cir. 2002). And it does not apply when an affidavit is so bare bones that an officer’s reliance on the warrant was unreasonable. *Payne*, 341 F.3d at 399–400.

Here, the good-faith exception applies. And because the warrant does not present a novel question of law, the Court need not determine whether probable cause supported the warrant. *Id.*

The good-faith exception applies because TFO Poor’s reliance on the warrant was objectively reasonable, his affidavit was not bare bones, and it contained no falsehoods. TFO Poor’s affidavit contained detailed information on Freenet and how law enforcement has investigated CSAM on Freenet since 2011. It described the algorithm law enforcement uses to identify the IP address that likely requested a download of CSAM.<sup>3</sup> It offered access to the peer-reviewed paper explaining the algorithm. It also listed six instances when Jordan’s IP address requested pieces of files known to be

---

<sup>3</sup> TFO Poor’s description of the algorithm and its error rate, which the Court detailed above, rebuts Jordan’s claim that TFO Poor’s affidavit was like basing “probable cause on a confidential informant without going into detail as [to] the informant’s basis of knowledge nor known reliability.” See Doc. 42, Reply, 2.

CSAM and explained how TFO Poor identified the person using his IP address and his physical address. *See generally* Doc. 34, Affidavit. The affidavit also notes that dozens of similar law enforcement searches on Freenet have found evidence of CSAM. *Id.* at 15. TFO Poor included sufficient details that he could reasonably and in good faith rely on the resulting warrant. Moreover, these details rebut Jordan's claim that the affidavit was bare bones. *See* Doc. 34, Mot., 14. Finally, as the Court discussed above, the affidavit did not contain falsehoods or material omissions.

And because the warrant does not raise a novel question of law, the Court need not determine whether probable cause supported the warrant. *See Payne*, 341 F.3d at 399. Jordan asserts his challenge to the algorithm presents "a matter of first impression in this district and the Fifth Circuit." Doc. 34, Mot., 12. But while it may present a *matter* of first impression, it does not present a *novel question of law*. Jordan contends that material omissions about the algorithm used to identify him as someone requesting CSAM precluded a finding of probable cause. *See generally id.* Thus, "the only question is whether or not the affidavit in question alleged sufficient facts to obtain a search warrant." *United States v. Kleinkauf*, No. 4:10-CR-13, 2010 WL 3781882, at \*1-2 (E.D. Tex. Sept. 20, 2010), *aff'd*, 487 F. App'x 836 (5th Cir. 2012). Accordingly, this does not present a novel question of law. Because the good-faith exception applies, the Court need not determine whether there was probable cause. The Court denies Jordan's Motion to Suppress.


#### IV.

#### CONCLUSION

For the foregoing reasons, Jordan's Motion to Suppress and Motion for a *Franks* Hearing (Doc. 34) is **DENIED**.

SO ORDERED.

SIGNED: July 10, 2025.



---

JANE J. BOYLE  
UNITED STATES DISTRICT JUDGE